Frequently Asked Questions

FAQ answers are available for the topics below. Please contact us to provide feedback about this page.

Introduction

What is CVE?

CVE is a dictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, databases, and services) with these definitions. CVE Entries are comprised of an identification number, a description, and at least one public reference.

What is the relationship between CVE and the NVD (U.S. National Vulnerability Database)?

See CVE and NVD Relationship.

Who owns CVE?

CVE is sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Operating as DHS's Federally Funded Research and Development Center (FFRDC), MITRE has copyrighted the CVE List for the benefit of the community in order to ensure it remains a free and open standard, as well as to legally protect the ongoing use of it and any resulting content by government, vendors, and/or users. In addition, MITRE has trademarked ® the CVE acronym and the CVE logo to protect their sole and ongoing use by the CVE effort within the cybersecurity arena.

Is CVE intended for public use? How can CVE help me?

CVE is free to use and publicly available to anyone interested in correlating data between different vulnerability or security tools, repositories, and services. You may search or download CVE, copy it, redistribute it, reference it, and analyze it, provided you do not modify CVE itself. You may also link to specific CVE Entry pages from your website, product, publication, or other capability. See the terms of use.

CVE helps because it provides a standardized identifier for a given vulnerability or exposure. Knowing this common identifier allows you to quickly and accurately access information about the problem across multiple information sources that are compatible with CVE. For example, if you own a security tool whose reports contain references to CVE IDs, you may then access fix information in a separate database that is compatible with CVE. CVE also provides you with a baseline for evaluating the coverage of your tools. With CVE's common identifiers, you'll know exactly what each tool covers allowing you to determine which tools are most effective and appropriate for your organization's needs.

In addition, if the security advisories your organization receives are compatible with CVE, you can see if your vulnerability scanners check for this threat and then determine whether your intrusion detection system has the appropriate attack signatures to identify attempts to exploit particular vulnerabilities. If you build or maintain systems for customers, the CVE compatibility of advisories will help you to directly identify any fixes from the vendors of the commercial software products in those systems (if the vendor fix site is compatible with CVE).

Why CVE? Is there a lot of support for something like this?

Using a common identifier makes it easier to share data across separate databases, tools, and services, which until the creation of CVE in 1999, were not easily integrated. If a report from a security capability incorporates CVE Entries, you may then quickly and accurately access fix information in one or more separate CVE-compatible tools, services, and repositories to remediate the problem. With CVE, your tools and services can "speak" (i.e., exchange data) with each other. You'll know exactly what each covers because CVE provides you with a baseline for evaluating the coverage of your tools. This means you can determine which tools are most effective and appropriate for your organization's needs. In short, CVE-compatible tools, services, and databases will give you better coverage, easier interoperability, and enhanced security.

CVE is industry-endorsed by the CVE Numbering Authorities (CNAs), CVE Board, and the numerous organizations that include CVE Entries in their products, services, and

vendor alerts and security advisories.

Isn't CVE just another vulnerability database?

No. CVE is not a vulnerability database. CVE is designed to allow vulnerability databases and other capabilities to be linked together, and to facilitate the comparison of security tools and services. As such, CVE does not contain information such as risk, impact, fix information, or detailed technical information. CVE only contains the standard identifier number with status indicator, a brief description, and references to related vulnerability reports and advisories. (Note: The U.S. National Vulnerability Database (NVD) provides fix, scoring, and other information for CVE Entries on the CVE List.)

Can't hackers use this to break into my network?

Any public discussion of vulnerability information may help a hacker. However, there are several reasons why the benefits of CVE outweigh its risks:

- CVE is restricted to publicly known vulnerabilities and exposures.
- For a variety of reasons, sharing information is more difficult within the cybersecurity community than it is for hackers.
- It takes much more work for an organization to protect its networks and fix all possible holes than it takes for a hacker to find a single vulnerability, exploit it, and compromise the network.
- Community opinion supports sharing information, reflected in the CVE Board and CVE Numbering Authorities (CNAs) as both include key organizations in cybersecurity.

What is a "vulnerability"? What is an "exposure"?

See Section 7.1: What Is a Vulnerability? of the *CVE Numbering Authority (CNA) Rules*.

Community

How can my organization and I be involved?

- Network Security Administrators/Policy and Decision Makers—Adopt products and services that are compatible with CVE or encourage your vendors to be CVE-compatible to support your enterprise requirements.

- Security Vendors/Vulnerability Database Managers/Service Providers—Deliver tools, databases, or services that are compatible with CVE to your customers for better coverage, easier interoperability, and enhanced security across the enterprise.

  Become a CVE Numbering Authority (CNA).

- Software Vendors—Incorporate the use and reservation of CVE Entries into your vulnerability handling process so that your customers can work with concise information and leverage the power of vulnerability scanners to verify that updates and fixes have been applied.

  Become a CVE Numbering Authority (CNA).

- Vulnerability Researchers/Software Vendors—Incorporate the use and reservation of CVE Entries into your initial public announcement of a vulnerability to ensure that the CVE ID number is instantly available to all CVE users and makes it easier to track vulnerabilities over time.

  Become a CVE Numbering Authority (CNA).

PRODUCT/SERVICE COMPATIBILITY

What does it mean for a product or service to be compatible with CVE?

Compatible with CVE means that a tool, website, database, or other security product or service uses CVE Entries in a manner that allows it to be cross-referenced with other products that employ CVE Entries.

Different tools provide different coverage/cross-referencing of CVE Entries (e.g., some tools might cover Unix, while others cover Windows). You will need to evaluate any CVE-compatible products and services based upon your organization's specific requirements.

How do I make my product or service compatible with CVE?

See CVE Compatibility Guidelines.

How can my organization register our product or service as compatible with CVE?

The previous CVE Compatibility Program of declarations and questionnaires has been discontinued and its product listings have been moved to "archive" status. The CVE Team will no longer accept declarations or questionnaires. Instead, a CVE

Compatibility Guidelines document has been provided to assist you in making your product or service compatible with CVE.

SPONSOR

Who sponsors CVE? What is the relationship between CVE and DHS?

CVE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). In addition, US-CERT, which is also sponsored by CISA, incorporates CVE IDs into its security advisories whenever possible and advocates the use of CVE, and products and services that are compatible with CVE, to the U.S. government and all members of the cybersecurity community.

MITRE'S ROLE

What is MITRE's role in CVE?

The MITRE Corporation (MITRE) currently manages and maintains the CVE List and this website, oversees the CVE Numbering Authorities (CNAs) and CVE Board, conducts community outreach activities, and provides neutral guidance throughout the process to ensure that CVE serves the public interest.

In addition, the MITRE CVE Team currently functions as the CVE Program Root CNA.

CVE Board

Who is the CVE Board?

The CVE Board includes numerous cybersecurity-related organizations including commercial security tool vendors, academia, research institutions, government departments and agencies, and other prominent security experts, as well as end-users of vulnerability information. Through open and collaborative discussions, the Board provides critical input regarding the data sources, product coverage, coverage goals, operating structure, and strategic direction of the CVE Program.

Refer to the CVE Board page for additional information, and a complete list of current members.

Are Board discussions public?

Yes, please see:

- Email Discussion Archives
- Meeting Archives

Is there a Board charter?

Yes, please see the CVE Board Charter.

How are new members added to the Board?

Please see Selection of Board Members in the CVE Board Charter for additional information.

CVE Numbering Authority (CNA)

What is a CVE Numbering Authority (CNA)?

A CVE Numbering Authority (CNA) is an organization that distributes CVE IDs to researchers and information technology vendors for inclusion in first-time public announcements of new vulnerabilities, without directly involving the CVE Team in the details of the specific vulnerabilities.

Visit Participating CNAs Types of CNAs, Growth of CNA Program Worldwide to see the number and types of participating CNAs from around the world.

To review the products covered by each CNA, and contact information, visit the Participating CNAs section on the Request a CVE ID page.

Is there a "How-To" manual for CNAs?

See documentation for CNAs.

How do we request blocks of CVE IDs using the web form?

Please see Requesting Blocks of CVE IDs (for CNAs only).

How can my organization become a CNA?

See How to Become a CNA.

CVE Entries

CVE ID BASICS

What is a CVE Entry?

A CVE Entry is an item in the CVE List. Each CVE Entry includes the following:

- CVE ID with four or more digits in the sequence number portion of the ID (i.e., "CVE-1999-0067", "CVE-2014-12345", "CVE-2016-7654321").
- Brief Description of the security vulnerability or exposure.
- Any pertinent References (i.e., vulnerability reports and advisories).

What is a CVE ID?

A CVE ID is the number portion of a CVE Entry, for example, "CVE-1999-0067", "CVE-2014-12345", and "CVE-2016-7654321".

CVE IDs are used by cybersecurity product/service vendors and researchers as a standard method for identifying vulnerabilities and for cross-linking with other repositories that also use CVE IDs. See About CVE Entries for additional information.

What is the CVE ID syntax and when did it change?

CVE ID syntax defines the ID number component of a CVE Entry, for example, "CVE-2014-9999999", which includes the CVE prefix + year + sequence number digits.

With the new syntax, CVE IDs can now have 4 or more digits in the sequence number portion of the ID. For example, CVE-YYYY-NNNN with 4 digits in the sequence number, CVE-YYYY-NNNNN with 5 digits in the sequence number, CVE-YYYY-NNNNNNN with 7 digits in the sequence number, and so on.

The change was necessary because the CVE ID syntax used since the inception of CVE in 1999, CVE-YYYY-NNNN, only supports a maximum of 9,999 unique identifiers

per year. Due to the ever increasing volume of public vulnerability reports, the CVE Board and CVE Team determined that the CVE Program needed to change the syntax of its standard vulnerability identifiers so that CVE can track more than 10,000 vulnerabilities in a single year. The new CVE ID syntax was determined in a vote by the CVE Board, details of which are available in the CVE Board Discussion List Archives.

The CVE ID Syntax Change took effect on January 1, 2014, and CVE IDs using the new syntax were first issued on January 13, 2015.

Please see CVE ID Syntax Change (Archived) and Technical Guidance for Handling the New CVE ID Syntax (Archived) for additional information.

What is the significance and meaning of the YEAR portion of a CVE ID

CVE IDs have the format CVE-YYYY-NNNNN. The YYYY portion is the year that the CVE ID was assigned OR the year the vulnerability was made public (if before the CVE ID was assigned).

The year portion is not used to indicate when the vulnerability was discovered, but only when it was made public or assigned.

Examples:

- A vulnerability is discovered in 2016, and a CVE ID is requested for that vulnerability in 2016. The CVE ID would be of the form "CVE-2016-NNNN".
- A vulnerability is discovered in 2015 and made public in 2016. If the CVE ID is requested in 2016, the CVE ID would be of the form "CVE-2016-NNNNN".
- A vulnerability is discovered in 2015 and a request is made for a CVE ID in 2015. The vulnerability is assigned "CVE-2015-NNNN" but not made public. (The CVE ID would appear as "Reserved" in the CVE List.) The discloser does not publish the CVE ID publicly until 2017, though. In this case, the CVE ID is still "CVE-2015-NNNN", despite the fact that the vulnerability isn't made public until 2017.
- A vulnerability is discovered and published in 2015 without having a CVE ID assigned to it. Someone requests that a CVE ID be assigned to the vulnerability in 2016. The vulnerability is given "CVE-2015-XXXX" since it was first made public in 2015.

NOTE: Neither the date when a vulnerability was introduced into a product, or the date when a vulnerability was fixed in a product, factor into what year is indicated in the CVE ID assigned to that vulnerability.

How are the CVE Entry DESCRIPTIONS created or compiled?

The "Description" portion of CVE Entries are typically written by CVE Numbering Authorities (CNAs), the CVE Team, or individuals requesting a CVE ID.

Descriptions should be unique and provide the relevant details to help users (1) find the CVE Entry for a specific vulnerability, and/or (2) distinguish between similar-looking vulnerabilities.

Ideally, Descriptions include details such as the name of the affected product and vendor, a summary of affected versions, the vulnerability type, the impact, the access that an attacker requires to exploit the vulnerability, and the important code components or inputs that are involved.

However, if this information is not available to the submitter of a CVE Entry, not all Descriptions will include all these details. For example, to write a CVE Description, the CVE Team analyzes public, third-party reports of vulnerabilities (i.e., "references"); extracts the relevant information from each reference; resolves any conflicting information or inconsistent usage of terminology; and then writes the description. In this example, the CVE Team only has access to publicly available information which may not include all the details of the ideal Descriptions.

Are there REFERENCES available for CVE Entries?

Each CVE Entry includes appropriate References. Each reference used in CVE (1) identifies the source, (2) includes a well-defined identifier to facilitate searching on a source's website, and (3) notes the associated CVE ID.

Per Appendix B: CVE Information Format of the CNA Rules document, which specifies requirements for References for CVE Entries: “References should point to content that is relevant to the vulnerability and include at least all the details included in the CVE Entry. Ideally, references should point to content that includes the CVE ID itself whenever possible. References must also be publicly available.”

References are valid as of the date the CVE Entry is published to the CVE List. Over time, if a Reference uniform resource locator (URL) stops working, the URL will be retained for historical purposes. To request that an additional Reference be added to a CVE Entry, go to the CVE Request web form and select "Request an update to an existing CVE Entry" from the dropdown menu.

What does DATE ENTRY CREATED signify in a CVE Entry?

The "Date Entry Created" date in a CVE Entry indicates when the CVE ID was issued to a CVE Numbering Authority (CNA) or the CVE Entry published on the CVE List.

This date does not indicate when the vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE. That information may or may not be included in the description or references of a CVE Entry, or in the enhanced information for the CVE Entry that is provided in the U.S. National Vulnerability Database (NVD).

Also see: FOCUS ON: The Significance and Meaning of the Year Portion of a CVE ID.

Do CVE Entries cite the discoverers of the vulnerabilities?

The CVE Program does not credit persons or organizations that discover vulnerabilities.

STATES OF CVE ENTRIES

What does it mean when a CVE Entry is marked "RESERVED"?

A CVE Entry is marked as "RESERVED" when it has been reserved for use by a CVE Numbering Authority (CNA) or security researcher, but the details of it are not yet populated. A CVE Entry can change from the RESERVED state to being populated at any time based on a number of factors both internal and external to the CVE List. Once the CVE Entry is populated with details on the CVE List, it will become available in the U.S. National Vulnerability Database (NVD). As one of the final steps in the process, the NVD Common Vulnerability Scoring System (CVSS) scores for the CVE Entries are assigned by the NIST NVD team.

What does it mean when a CVE Entry is marked "DISPUTED"?

When one party disagrees with another party's assertion that a particular issue in software is a vulnerability, a CVE Entry assigned to that issue may be designated as being "DISPUTED". In these cases, CVE is making no determination as to which party is correct. Instead, we make note of this dispute and try to offer any public references that will better inform those trying to understand the facts of the issue.

When you see a CVE Entry that is "DISPUTED", we encourage you to research the issue through the references or by contacting the affected vendor or developer for more information.

What does it mean when a CVE Entry is marked "REJECT"?

A CVE Entry listed as "REJECT" is a CVE Entry that is not accepted as a CVE Entry. The reason a CVE Entry is marked REJECT will most often be stated in the description of the CVE Entry. Possible examples include it being a duplicate CVE Entry, it being withdrawn by the original requester, it being assigned incorrectly, or some other administrative reason.

As a rule, REJECT CVE Entries should be ignored.

However, there may be cases where a CVE Entry previously marked as REJECT might need to move back to RESERVED or a populated state (i.e., the details and References are published and included). An example case could include a simple accidental REJECT, where a CVE Entry was marked as REJECT by a CVE Numbering Authority (CNA) but the CVE ID was used publicly. In this case, it would create more confusion and additional work to REJECT the already used CVE ID, assign a new CVE ID, and also make sure that all public references are updated. The change discussed here would be to simply change the REJECT CVE Entry and populate it with the details that were intended.

Also see: FOCUS ON: Marking a CVE ID “REJECT” Is Not Permanent; It Can Be Updated and Added to the CVE List.

Why is a CVE Entry marked as "RESERVED" when a CVE ID is being publicly used?

A CVE Entry is marked as "RESERVED" when it has been reserved for use by a CVE Numbering Authority (CNA) or security researcher, but the details of it are not yet populated. Often, this is because the original requester of the CVE ID assignment has not sent an update to the CVE Team including the information needed to populate

the CVE Entry. Note that a CVE Entry cannot be populated with details until a public reference exists that describes the vulnerability in question.

If you are aware of a CVE ID that is being used publicly but is not yet included in the CVE List (i.e., CVE Entry is still marked as RESERVED), or you have additional information for an already populated CVE Entry, you can request that the CVE Entry be updated through the CVE Request web form.

UPDATING INFORMATION IN CVE ENTRIES

How can I update existing information or add new information to a CVE Entry Description or Reference?

See Update a CVE Entry.

REQUESTING NEW CVE IDs

How can I obtain a CVE ID?

See Request a CVE ID.

CVE List Basics

Does the CVE List contain all vulnerabilities and exposures?

The intention of CVE is to be comprehensive with respect to all publicly known vulnerabilities and exposures. And while CVE prioritizes the assignment of CVE Entries for the products, vendors, and product categories listed on the Request a CVE ID page, a CVE ID may be requested for any vulnerability.

Where does CVE find out about these vulnerabilities and exposures?

CVE IDs are assigned by CVE Numbering Authorities (CNAs) from around the world. As CVE Program Root CNA, the CVE Team also accepts requests for CVE IDs. Please see Request a CVE ID for details.

How does a vulnerability or exposure become a CVE Entry?

The process begins with the discovery of a potential security vulnerability or exposure. The information is then assigned a CVE ID by a CVE Numbering Authority (CNA), the CNA writes the Description and adds any References, and then the completed CVE Entry is posted on the CVE website by the CVE Team.

Generally, the CVE approach is to create separate CVE Entries for independently fixable vulnerabilities, except when they are the result of a shared codebase, library, protocol, or standard. CVE List Rules and Guidance, which are the guidelines the CVE Program uses to ensure that CVE Entries are created in a consistent fashion, independent of which CNA is doing the creation, include the following: CVE Counting Rules, CVE Information Format, and Process to Correct Counting Issues.

Why doesn't CVE include fix information, impact, classification, or other important technical details?

This information can already be found in numerous vulnerability websites, databases, and security tool databases. CVE doesn't have this information because CVE is intended to link these different vulnerability capabilities, not to replace them.

Note: The U.S. National Vulnerability Database (NVD) provides fix and other information for entries on the CVE List.

Why doesn't CVE use a taxonomy?

Developing a universally applicable taxonomy for vulnerabilities is an ongoing area of research. One goal of CVE is to capture community agreement. The enumeration and categorization of vulnerabilities are different (albeit related) efforts. The effort of building and populating the CVE List may facilitate further advances in the study of vulnerability taxonomies.

Are there release versions of the CVE List?

No. The most current version of the CVE List is available on the CVE List page.

Why did CVE retire the term CVE "candidates"?

When the CVE effort first began in 1999 and vulnerabilities were discovered and published less frequently than they are today, CVEs were issued "candidate" or "entry" status, where candidate status indicated that the identifier was under review for inclusion on the CVE List and entry status indicated that the identifier has been formally accepted to the list. CVEs with candidate status used the CAN-prefix (e.g., "CAN-1999-0067"), while CVEs with entry status used the CVE-prefix (e.g., "CVE-1999-0067"). This meant that the individual identifier numbers themselves would need to be changed once a candidate had been updated to entry status, placing a significant burden on the numerous vendors and organizations around the world that would in turn need to update their tools and processes to accommodate the replacement identifier numbers. This became especially burdensome as the volume of vulnerabilities being discovered and added to the CVE List increased dramatically each year (CVE Entries are now added to the CVE website on a daily basis). Therefore, at the request of the community, as of 2005 all CVE Entries now use the CVE-prefix and are immediately usable by the community. While references and

other supporting information may be updated over time, the CVE ID itself does not change once it has been assigned to an issue.

Does CVE have a data feed of new CVE Entries?

Yes, see CVE Data Feeds.

Does the CVE List include severity ratings (i.e., CVSS scores) for CVE Entries?

No, the CVE List does not include severity ratings for CVE Entries.

However, severity scores for CVE Entries are provided by the U.S. National Vulnerability Database (NVD) at https://nvd.nist.gov/cvss.cfm.

Using the CVE List

Someone has hacked into my website. Can CVE help me recover?

CVE cannot help you to determine precisely what vulnerability an attacker may have exploited to obtain unauthorized access. But once you determine what vulnerability was exploited, you could find the CVE ID and use it to examine information sources that are compatible with CVE in order to obtain fix information, technical details, and other information that will be helpful to you.

How can CVE help me protect my network?

By using the CVE ID for a particular vulnerability or exposure, you will be able to quickly and accurately obtain information from a variety of information sources that are compatible with CVE. By facilitating better comparisons between different security tools and services, CVE can help you make a better choice as to which of these capabilities are appropriate for your needs. You may also be able to create a

suite of interoperable security tools and capabilities from multiple vendors, if those tools and capabilities incorporate CVE as a translation mechanism.

Using products and services that are compatible with CVE will allow you to improve how your organization responds to security advisories. If the advisory includes CVE ID, you can see if your scanners or security service checks for this threat and then determine whether your intrusion detection system has the appropriate attack signatures. If you build or maintain systems for customers, the CVE compatibility of advisories will help you to directly identify any fixes from the vendors of the commercial software products in those systems (if the vendor fix site is compatible with CVE).

Other indirect benefits may also arise from CVE. For example, it facilitates better research on vulnerabilities and exposures.

What types of products and services include CVE Entries or reference CVE IDs?

CVE Entries and CVE IDs are used in a variety of cybersecurity-related products and services including: security advisories; vulnerability databases; vulnerability and security websites; vulnerability assessment, notification, and remediation; intrusion detection and management; intrusion monitoring and response; data/event correlation; firewalls; incident management; security information management; policy compliance; patch management; etc.

How will CVE help me compare security tools?

With CVE, your vulnerability databases, services, and tools can "speak" to each other. Until the creation of CVE in 1999 it was very difficult to effectively decide which tool was the most appropriate for an organization's needs. Each vendor used a different definition of "vulnerability" or "exposure" and used different metrics to state how many vulnerabilities or exposures they "check" or "test." CVE provides vendors with a standard list they can compare to, thus allowing you to compare apples to apples. CVE may also be useful for obtaining quantitative data on tool behaviors, such as how they perform their checks, the impact they have on the systems they examine, the rate of false positives or false negatives, or how quickly they update their tools when new entries are introduced into CVE.

Can I include CVE IDs in my product/database/security advisory/etc.?

Yes, CVE is free to use. You may search or download the CVE List, copy it, redistribute it, reference it, and analyze it, provided you do not modify CVE itself. You may also link to specific CVE Entry pages from your website, product, publication, or other capability. See the Terms of Use.

Is CVE content available in Common Vulnerability Reporting Framework (CVRF) format?

Yes, CVE content can be downloaded in Common Vulnerability Reporting Framework (CVRF) format on the Download CVE page. A single download of all CVE entries in CVRF format is available, as are downloads for individual calendar years in CVRF format such as 2017, etc. Visit the CVE Usage of CVRF page to learn more.

Are CVE Entries mapped to IAVAs?

Yes, CVE Entries are mapped to the U.S. Defense Information System Agency's (DISA) Information Assurance Vulnerability Alerts (IAVAs). DoD PKI Certificates are required to access the information. For details, contact DISA.

How do I download a copy of CVE?

See Download CVE.

How do I search CVE?

Visit Search CVE to search the CVE List by keyword(s) or by CVE ID.

Other free CVE List search resources are also available.

Also, as part of it's enhanced CVE List content, the U.S. National Vulnerability Database (NVD) provides advanced searching features such as by OS; by vendor name, product name, and/or version number; and by vulnerability type, severity, related exploit range, and impact.

Can I search CVE by operating system?

No. The CVE search was designed to help identify specific vulnerabilities and exposures, and not to find sets of problems that share common attributes such as operating systems. Therefore, you should not search CVE by operating system because your results will be incomplete.

Note: The U.S. National Vulnerability Database (NVD), which is based upon and synchronized with the CVE List, is searchable by operating system.

I searched CVE and I got two or more results back. How can I tell which is the one I want?

While the description for a CVE Entry should be able to uniquely identify a vulnerability or exposure, they are intentionally brief, and in some instances you may need to rely on the accompanying References to make a determination. When this occurs it is either because not enough details about the problem were originally provided, because the Description includes unique details that you may not be familiar with, or because of an error in the Description itself. In addition to referring to the References, you could also search through websites that are compatible with CVE by specifying the CVE Entries that you are uncertain about.

Note: The U.S. National Vulnerability Database (NVD) provides fix and other information for entries on the CVE List.

CVE Request Web Form

WEB FORM BASICS

How do I get to the CVE Request web form?

The CVE Request web form is available at https://cveform.mitre.org.

Why should I use the web form?

The CVE Team assigns tickets to all new requests submitted via the CVE Request web form, which allows us to better track and manage the requests than if they were submitted through some other means.

Please use the web form for:

- Requesting CVE ID(s) from the CVE Team
- Requesting a block of CVE IDs (for CVE Numbering Authorities (CNAs) only)
- Requesting an update to a CVE Entry
- Providing notification about a vulnerability publication
- Submitting comments

Once you have submitted your request, you will receive an email confirming receipt of your request and a reference number. Any additional communications related to that request will be done through email using the same subject line as the confirmation email.

Where can I find additional help using the web form?

In addition to these CVE Request web form FAQs, additional help and user guidance are available in the following locations:

- Web Form Online Help – On the web form itself, click the information button (round, blue icon containing the letter "i") next to the parts of the form in which you require additional information.
- Web Form Overview – A high-level presentation of how to use the CVE Request web form to request CVE IDs from the CVE Program Root CNA, request an update to an existing CVE entry, provide notification about a vulnerability publication, or submit comments or questions.
- Web Form User Tips – Information and tips for using each of the CVE Request web forms: Request a CVE ID; Request a block of IDs (for CNAs only); Notify CVE about a publication; Request an update to an existing CVE; and Other.

Finally, you may also choose the "Other" request type on the CVE Request web form itself and enter any questions you have into the free-text field. The CVE Team will receive this information and respond to your question(s) via email.

USING THE WEB FORM

What are the different choices for request type?

The choices for a request type are:

- Request a CVE ID
- Request a block of IDs (for CNAs only)
- Notify CVE about a publication
- Request an update to an existing CVE
- Other

How do I access the Product and Sources list when I am using the CVE Request web form?

Select the "Request a CVE ID" request type and, in the grey box, you will see a link to the products covered by the Participating CNAs.

What if I realized I entered something wrong? Can I edit the information I entered on the web form after I submit it?

No, you cannot edit the form once it has been submitted; however, after submitting the web form, you will receive an email confirmation with a reference number, and you can reply to that email with any changes. Do not modify the subject line, as it contains the reference number associated with your request.

Can I add an attachment?

The web form does not accept attachments. However, in the event an attachment is necessary, it can be sent in a reply to the confirmation email you receive when you submit the form. Do not modify the subject line, as it contains the reference number associated with your request.

I have trouble seeing the security code, or CAPTCHA, at the end of the form. Is there any other way to submit my form?

The security code, or CAPTCHA, is required to complete the form. If you do not accurately type the CAPTCHA, you will receive an error message upon clicking the "Submit" button, along with a new CAPTCHA, which may be easier to view. If you continue to experience problems with the CAPTCHA, please contact us.

I don't understand the note after I submit my request that says I should close my browser and open it again. What does that mean? Should I do it?

If you submit multiple requests in the same browser session, all requests will share a reference number and a single confirmation email will be sent (in response to the first request). If your requests are related, and need to be tracked together, you do not need to close your browser. If you refresh your browser or close and reopen your browser between each request, you will receive a new confirmation email and reservation number for each request.

What if I need more than 10 CVE IDs?

You can use the CVE Request web form to request up to 10 CVE IDs. If you need to request more than 10 CVE IDs, you can do so by submitting another request. CNAs, please see: How do we request blocks of CVE IDs using the web form?

User Tips:

- If you cannot type a new number into the field for entering the number of CVE IDs you are requesting, use backspace or the delete key to first clear the highlighted default number and then enter your desired number.
- All requests within a single browser session will share a single reference number and will only receive a confirmation email for the first request. If you refresh your browser or close and reopen your browser between each request, you will receive a new confirmation email and reservation number for each request.

Why does the form get so big when I request more than one CVE ID?

When you request more than one CVE ID on the CVE Request web form, a separate set of required/optional fields for each of the CVE IDs requested is added, which causes the form to expand.

How can I encrypt my requests via the web form?

If you need to encrypt the details of your request, please enter your public PGP key into the "Enter a PGP Key" dialog box. If your PGP key is longer than 20,000

characters, please provide a URL for your PGP. If you do not have a URL, please contact us to identify an alternative suggestion. Provide generic details in the form as needed. The CVE Team will use the PGP key you provided to begin an encrypted dialogue with you via email.

AFTER SUBMITTING YOUR WEB FORM REQUEST

How do I know that my CVE request has been received?

You will receive an email confirmation once you submit the form, along with a reference number. If you later have any additional information to provide, please reply to that email. Do not modify the subject line, as it contains the reference number associated with your request.

Please note that all requests within a single browser session will share a single reference number and will only receive a confirmation email for the first request. If you refresh your browser or close and reopen your browser between each request, you will receive a new confirmation email and reservation number for each request.

User Tip: Please add cve-request@mitre.org and cve@mitre.org as safe senders in your email client before completing the form.

What if I realize, after submitting the form, that I need to request more CVE IDs?

You are able to complete the CVE Request web form as often as needed. If you submit a new request in the same browser session, all requests will share a reference number and a single confirmation email will be sent (in response to the first request). If you refresh your browser or close and reopen your browser between each request, you will receive a new confirmation email and reservation number for each request.

What do I do if I need to follow up on a request made through the CVE Request web form that has not been completed?

For requests that have not yet been completed (e.g., a CVE ID has not yet been assigned in response to a CVE ID request), you can provide additional information by replying to the confirmation email you received when you submitted the web form. Do not modify the subject line, as it contains the reference number associated with your request.

How do I know when my request has been fulfilled? Is there a place I can look online to see a status?

Status updates are not available via the website or web form. Once you submit the web form, all further communication regarding the request and its status takes place via email, with the same subject line that was in the original confirmation email. Requesters will be notified when their request is fulfilled. If a request was not fulfilled, the requester will receive an email notifying them of the decision and rationale (see My request for CVE IDs was rejected. How do I follow up?).

My request for CVE IDs was rejected. How do I follow up?

If you would like the CVE Team to reconsider a rejected request, please use the CVE Request web form to submit an "Other" request and include both the reference number of your original request and additional information that should be considered.